



UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/458,921	12/10/1999	MOHAMMAD PEYRAVIAN	P-4541.001	9480

24112 7590 10/17/2005
COATS & BENNETT, PLLC
P O BOX 5
RALEIGH, NC 27602

EXAMINER

MOORTHY, ARAVIND K

ART UNIT PAPER NUMBER

2131

DATE MAILED: 10/17/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/458,921	Applicant(s) PEYRAVIAN ET AL.	
	Examiner Aravind K. Moorthy	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 25 July 2005.
- 2a) This action is **FINAL**.
- 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-50 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) 1-28 and 47-50 is/are allowed.
- 6) Claim(s) 29-46 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 10 December 1999 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 - 1. Certified copies of the priority documents have been received.
 - 2. Certified copies of the priority documents have been received in Application No. _____.
 - 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) Notice of Informal Patent Application (PTO-152)
- 6) Other: _____.

DETAILED ACTION

1. This is in response to the appeal brief filed on 25 July 2005.
2. Claims 1-50 are pending in the application.
3. Claims 29-46 have been rejected.
4. Claims 1-28 and 47-50 have been allowed.

Response to Arguments

5. Applicant's arguments filed 25 July 2005 have been fully considered but they are not persuasive.

On page 13, the applicant argues that the MAC is a one-way hash function that includes the secret key.

The examiner asserts that nowhere in claim 29 is it claimed that the MAC is a one-way hash function that includes the secret key.

On page 13, the applicant argues that Levine does not generate a MAC as called out in claim 29.

The examiner respectfully disagrees. Claim 29 recites generating a MAC based on the time stamp and a secret key. The manner in which the MAC is created is not claimed. Levine does teach generating a form of a MAC based on the time stamp and a secret key.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 29-46 are rejected under 35 U.S.C. 102(e) as being anticipated by Levine U.S. Patent No. 6,393,566 B1.

As to claim 29, Levine discloses a method for time stamping a document comprising:

- a. receiving a time stamp request at an outside agency at a first time, the time stamp request including identifying data associated with the document [column 3, lines 54-67];
- b. creating at the outside agency a time stamp receipt based on the identifying data and a time indication [column 3, lines 41-53]; and
- c. generating at the outside agency a message authentication code based on the time stamp receipt and a secret key [column 4, lines 22-28]; and
- d. transmitting the time stamp receipt and the message authentication code to the requestor [column 5, lines 39-65].

As to claim 30, Levine discloses that the identifying data comprises a digital representation of at least a portion of the document [column 5, lines 39-65].

Art Unit: 2131

As to claim 31, Levine discloses that the identifying data comprises a digital sequence derived by application of a deterministic function to at least a portion of the document [column 5, lines 39-65].

As to claim 32, Levine discloses that the digital sequence is a hash value derived by application of a one-way hashing function to at least a portion of the document [column 5, lines 39-65].

As to claim 33, Levine discloses that the time stamp receipt includes a copy of at least a portion of the identifying data concatenated with the time indication [column 5, lines 39-65].

As to claim 34, Levine discloses that the time stamp receipt includes a digital sequence derived from the identifying data concatenated with the time indication [column 3, lines 41-53].

As to claim 35, Levine discloses that the time stamp request further includes an identification number associated with the requestor [column 5, lines 25-37].

As to claim 36, Levine discloses that the message authentication code comprises a numeric representation generated by application of a deterministic function to the time stamp receipt and the secret key concatenated together [column 6, lines 9-29].

As to claim 37, Levine discloses generating a second message authentication code based on the first message authentication code and a second secret key [column 5, lines 39-65].

As to claim 38, Levine discloses transmitting the second message authentication codes to the requestor [column 6, lines 9-29].

As to claim 39, Levine discloses the step of encrypting the first secret key to generate an encrypted key [column 7 line 57 to column 8 line 9].

As to claim 40, Levine discloses transmitting the encrypted key to the requestor [column 7 line 57 to column 8 line 9].

As to claim 41, Levine discloses a method for time stamping documents comprising:

- a. receiving at an outside agency a certification request, the certification request including a time stamp receipt and a message authentication code generated on the time stamp receipt [column 4, lines 22-28];
- b. validating the message authentication code at the outside agency using a secret key [column 5, lines 12-38];
- c. certifying the time stamp receipt if the message authentication code is valid using a cryptographic signature scheme [column 5, lines 12-38].

As to claim 42, Levine discloses that the step of certifying the time stamp receipt includes signing the message authentication code at the outside agency using a cryptographic signature scheme [column 5, lines 12-23].

As to claim 43, Levine discloses that the step of certifying the time stamp record includes signing the time stamp receipt at the outside agency using a cryptographic signature scheme [column 5, lines 12-23].

As to claim 44, Levine discloses including the step of transmitting the certified time stamp receipt to the requestor [column 5, lines 39-65].

As to claim 45, Levine discloses that certifying the time stamp receipt at the outside agency comprises signing the time stamp receipt with a private signature key [column 5, lines 39-65].

Art Unit: 2131

As to claim 46, Levine discloses that certifying the time stamp receipt at the outside agency comprises signing the message authentication code with a private signature key [column 5, lines 39-65].

Allowable Subject Matter

7. Claims 1-28 and 47-50 are allowed.

As to claim 1, prior art does not disclose or fairly teach e. receiving a certification request at the outside agency at a second time, the certification request including the time stamp receipt and the message authentication code. Prior art does not disclose or fairly teach f. validating the message authentication code at the outside agency using the secret key. Prior art does not disclose or fairly teach g. certifying the time stamp receipt at the outside agency using a cryptographic signature scheme if the message authentication code is valid.

As to claim 15, prior art does not disclose or fairly teach d. encrypting the first secret key with a second secret key to generate a key message. Prior art does not disclose or fairly teach e. generating a second message authentication code based on the first message authentication code and the first secret key using a third secret key. Prior art does not disclose or fairly teach f. transmitting the time stamp receipt, the first message authentication code, the second message authentication code, and the end key message to the requestor. Prior art does not disclose or fairly teach g. receiving at the outside agency at a second time a certification request, the certification request including the time stamp receipt, the first message authentication code, the second message authentication code, and the encrypted key message. Prior art does not disclose or fairly teach h. decrypting at the outside agency the encrypted key message to recover the first secret key. Prior art does not disclose or fairly teach i. validating the second message

Art Unit: 2131

authentication code at the outside agency using the third secret key. Prior art does not disclose or fairly teach j. validating the first message authentication code at the outside agency using the first secret key if the second message authentication code is valid. Prior art does not disclose or fairly teach k. certifying the time stamp receipt at the outside agency using a cryptographic signature scheme if the first message authentication code is valid.

Any claims not directly addressed are allowed on the virtue of their dependency.

Conclusion

8. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

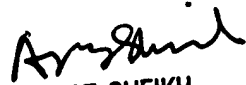
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

Art Unit: 2131

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy 
October 13, 2005


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100